Top 7 Fidelis Elevate® Integrations You Need to Know

In today's dynamic cybersecurity landscape, disconnected tools result in fragmented visibility, slower response, and higher risk. To stay ahead of threats, organizations need a connected defense architecture—where tools talk to each other, act intelligently, and minimize analyst fatigue.

That's exactly what **Fidelis Elevate® integrations** are designed to do.

Fidelis Elevate®, a robust Extended Detection and Response (XDR) platform, supports a wide range of out-of-the-box integrations with leading SOAR, SIEM, EDR, SSE, threat intelligence, and network tools. These integrations allow security teams to correlate, detect, and respond to threats across every layer of their IT environment—unifying visibility and streamlining operations.

Here are the **top 7 Fidelis Elevate® integrations** that every security team should explore.

1. SOAR Integrations: Automate and Accelerate Incident Response

Integrated with:

- Splunk SOAR
- Palo Alto Networks Cortex XSOAR
- D3 Security
- Respond Software

Why it matters:

Security Orchestration, Automation, and Response (SOAR) platforms that are used to automate repetitive tasks and enforce playbooks. Fidelis Elevate®'s SOAR integrations enable alerts and threat intelligence to trigger real-time automated actions, with zero delay and zero human error.

Example in action:

A lateral movement detection by Fidelis Elevate® can automatically trigger a Cortex XSOAR playbook. The system isolates the endpoint, raises an alert, and logs the event—all without human intervention.

2. SIEM Integrations: Aggregate Logs and Correlate Threats

Integrated with:

- Splunk
- IBM QRadar
- Devo

- HPE ArcSight

Why it matters:

Security Information and Event Management (SIEM) tools allow enterprises to aggregate log data across systems and correlate events to uncover potential threats. Fidelis Elevate® integrations ensure that enriched alerts, deep session metadata, and forensic details are shared with SIEMs—turning isolated alerts into actionable insights.

Example in action:

When Fidelis detects unusual outbound connections, it forwards this data to IBM QRadar. QRadar correlates the alert with failed login attempts and privilege escalation events—giving analysts the complete picture in one view.

3. Threat Intelligence Integrations: Add Real-Time Context

Integrated with:

- ReversingLabs
- McAfee
- SecondWrite

Why it matters:

Threat intelligence integration compounds Fidelis' ability to identify known and unknown threats. Fidelis Elevate® is able to contextualize alerts, validate suspicious behavior, and flag indicators that correspond to a target's emerging threat campaigns by taking advantage of real-time intel feeds.

Example in action:

A file flagged by Fidelis is instantly checked against ReversingLabs' threat database. If identified as malicious, the alert severity is raised, and automated remediation can be triggered through a SOAR system.

Know What You're Defending. Start with Fidelis Insight™

Map every asset, expose hidden risks, and take control.

- Discover assets across cloud and on-prem
- Spot unmanaged devices instantly
- Focus on high-impact vulnerabilities

Get the datasheet

4. EDR & Malware Protection Integrations: Close the Loop on Endpoint Threats

Integrated with:

- Carbon Black (VMware)
- Palo Alto NGFW

Why it matters:

While Fidelis delivers deep network and deception capabilities, integrating with endpoint and firewall tools expands coverage across attack surfaces. These integrations help in real-time containment, proactive blocking, and investigation from endpoint to perimeter.

Example in action:

If FireEye NX spots suspicious malware activity, Fidelis Elevate® analyzes related network traffic while instructing Carbon Black to quarantine the compromised host. Meanwhile, Palo Alto NGFW blocks further communication to the threat actor's IP.

5. Packet Broker Integrations: Deliver Network Visibility at Scale

Integrated with:

- Gigamon
- F5
- A10 Networks

Why it matters:

Packet brokers like Gigamon and F5 mirror, filter, and route traffic efficiently to security tools. Fidelis Elevate® integrations with these brokers ensure that no critical traffic is missed—even in high-throughput environments—without burdening performance.

Example in action:

Gigamon feeds segmented traffic into Fidelis sensors deployed at strategic junctions. This setup ensures even lateral east-west traffic is monitored—eliminating blind spots within internal networks.

6. EDR Integration with Fidelis Network: Deepen Endpoint Context

Integrated with:

- SentinelOne

Why it matters:

By integrating with SentinelOne, Fidelis Network® gains rich endpoint telemetry, including process execution, file access, and registry activity. This allows the platform to correlate network indicators with endpoint behavior—pinpointing threats faster and more accurately.

Example in action:

SentinelOne detects a suspicious PowerShell script. Fidelis Network® correlates this with unusual DNS activity to known malicious domains, helping the SOC team distinguish real threats from noise.

7. SSE Integration: Secure Cloud and Remote Access

Integrated with:

- Zscaler

Why it matters:

In a world of hybrid work and cloud-first applications, Secure Service Edge (SSE) platforms like Zscaler are essential. Fidelis Elevate® integrations with SSE solutions provide visibility into encrypted cloud-bound traffic, enforce policies, and detect exfiltration attempts from anywhere.

Example in action:

Zscaler sends cloud traffic logs to Fidelis for analysis. When Fidelis spots signs of sensitive data moving to unauthorized destinations, it triggers alerts and policy violations are flagged in real-time.

Why These Fidelis Elevate® Integrations Matter

These integrations deliver much more than connectivity — they are the foundation of intelligent, adaptive and unified security architecture. Whether it is through automating threat response, enhancing the detections with global intelligence or seeing the real-time view there on endpoints and cloud, Fidelis Elevate® integrations will help you build that layered defense.

Key benefits:

- **Consolidated threat visibility** from endpoint to network to cloud
- **Faster decision-making** through automation and contextual correlation
- **Proactive defense** with real-time threat intelligence feeds
- **Operational efficiency** by eliminating manual alert management
- **Scalability** without adding overhead or complexity

Conclusion: Powering the Modern SOC with Fidelis Elevate® Integrations

The SOC of today does not work in silos. It’s an integrated ecosystem where each tool has its purpose — automating response, enriching alerts, accelerating investigations, and controlling all things hybrid.

That vision is possible thanks to Fidelis Elevate® integrations. They enable teams to consolidate security operations across network, endpoint and cloud, so analysts have full visibility of threats and the ability to respond in real time. For those organizations seeking to enhance and modernize their detection and response strategy. They are the essential building blocks to an efficient, scalable, and intelligent defense posture.

Ready to See Fidelis Elevate in Action?
Explore how integrated defense transforms security operations.

- Connect with SOAR, SIEM, EDR & more
- Detect threats in real-time
- Automate response, reduce dwell time

Get a Demo